Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claims:

Claim 1. (Currently Amended) A method of decrypting encrypted content stored on a terminal, the method comprising the steps of:

receiving a request to access encrypted content on a terminal;

obtaining a license comprising a content decryption key and a set of binding attributes, the attributes including a public key of an authorized user of the encrypted content;

in response to the request, polling a personal trusted device of said user to digitally sign data with a private key associated with the device;

receiving said digitally signed data from said device; ~~and~~

verifying at the terminal the digitally signed data utilizing the public key; and wherein the terminal in response to verification of the digitally signed data uses the content decryption key to decrypt the encrypted content;

following said step of receiving said digitally signed data, applying a hashing algorithm to said data and decrypting said digitally signed data; and

comparing results of said application of said hashing algorithm with said decrypted data in said step of verifying.

Claim 2. (Original) A method as claimed in claim 1, comprising: encrypting at least the content decryption key.

Claim 3. (Original) A method as claimed in claim 2, wherein: encryption is performed using a public key of an asymmetric key pair such that decryption of the content decryption key is carried out using a private key of the asymmetric key pair.

Claim 4. (Original) A method as claimed in claim 3, wherein: the private key is stored in a tamperproof and secure location.

Claim 5. (Original) A method as claimed in claim 4, wherein: the secure location comprises a security element.

Claims 6-15. (Canceled)

Claim 16. (Currently Amended) A terminal for accessing encrypted content comprising:

a storage storing the encrypted content and a license, the license containing a content decryption key and a set of binding attributes, the attributes including a public key for a licensee of said content;

a digital rights management engine configured to:

receive a request to access said stored encrypted content from said licensee of said content;

generate identity verification data in response to said request;

establish, in response to said request, a communication link between the terminal and at least one other local terminal using a personal area network to request the other

local terminal to encrypt and digitally sign the identity verification data, generated by said terminal, using a private key stored at the other local terminal and assigned to said licensee of said content, wherein said other terminal is a mobile telephone of said licensee;

receive said digitally signed identity verification data from said other local terminal;

use said public key to decrypt said encrypted identity verification data; and

analyze said decrypted data to verify that the private key stored at the other local terminal corresponds to the public key in the license, and upon successful verification, decrypt the encrypted content using the content decryption key.

Claim 17. (Previously Presented) A terminal as claimed in claim 16, comprising: a secure storage for a private key of an asymmetric key pair; and wherein the controller is further configured to decrypt at least the content decryption key, the content decryption key having been encrypted using a public key of the asymmetric key pair.

Claim 18. (Original) A terminal as claimed in claim 17, wherein: the storage is provided by a security element.

Claim 19. (Previously Presented) A terminal as claimed in claim 16, wherein: the digitally signed identity verification data is delivered to the storage.

Claim 20. (Previously Presented) A terminal as claimed in claim 17, wherein: the digitally signed identity verification data is delivered to the storage.

Claim 21. (Previously Presented) A terminal as claimed in claim 18, wherein: the digitally signed identity verification data is delivered to the storage.

Claims 22-83 (Canceled)

Claim 84 (Previously Presented) A method of decrypting encrypted content stored on a terminal, the method comprising the steps of:

receiving a request to access encrypted content on a terminal;

obtaining a license comprising a content decryption key and a set of binding attributes, the attributes including a public key of an authorized user of the encrypted content;

in response to the request, polling a personal trusted device of said user to digitally sign data with a private key associated with the device, wherein said personal trusted device is a mobile telephone;

receiving said digitally signed data from said device; and

verifying at the terminal the digitally signed data utilizing the public key; and wherein the terminal in response to verification of the digitally signed data uses the content decryption key to decrypt the encrypted content.

Claim 85 (Previously Presented) The method of claim 1, wherein said personal trusted

device is communicatively coupled with said terminal via a wireless interface.

Claim 86 (Previously Presented) The method of claim 85, wherein said wireless interface is a low power radio frequency interface.

Claim 87 (Previously Presented) The method of claim 1, wherein said terminal is a rendering machine, and said method further includes a step of rendering said decrypted content on said rendering machine.

Claim 88 (Previously Presented) The method of claim 1, further comprising the steps of:

receiving an identification of a user making said request; and

comparing said identification with a public portion of said license.

Claim 89 (Previously Presented) The method of claim 88, further comprising the step of accessing public portions of a plurality of licenses stored on said terminal to locate a license corresponding to said user.

Claims 90-92 (Canceled)

Claim 93 (Previously Presented) The terminal of claim 16, wherein said identity verification data is a text string randomly generated by said other terminal.

Claim 94 (Canceled).

Claim 95 (Previously Presented) The method of claim 1, wherein said personal trusted device is located proximate to the terminal, and wherein said polling uses a personal area network to instruct said personal trusted device to digitally sign test verification data with a private key of the authorized user stored in said personal trusted device.

Claim 96 (Currently Amended) The method of claim 1, wherein said polling transmits to ~~one~~ two or more devices within a personal area network containing the terminal.

Claim 97 (Previously Presented) The method of claim 96, wherein said polling uses low power radio frequency transmission.

Claim 98 (Previously Presented) The method of claim 96, further comprising receiving polling responses from a plurality of devices located proximate to the terminal and connected to the personal area network.

Claim 99 (Previously Presented) The terminal of claim 16, further comprising:

a low power radio frequency interface, wherein said engine is further configured to use said low power radio frequency interface to establish said communication link with said other local terminal.

Claim 100 (Currently Amended) A digital rights management system, comprising:

a rendering terminal, said rendering terminal including:

a memory storing encrypted content and a license, said license including an exposed identity of a licensee to said content and an encrypted decryption content key;

a processor configured to receive a request to access said content and, in response to said request, perform the following:

transmit a polling request to a personal area network local to the terminal, said polling request requesting that a terminal receiving the request digitally sign test verification data using a private key stored on said terminal, said private key being assigned to said licensee;

receive a response to the polling request and determine whether said licensee is within a range of said personal area network, wherein said rendering terminal processor is further configured to generate said test verification data using a hashing algorithm; and

a mobile terminal, said mobile terminal including:

a memory storing a private key assigned to said licensee; and

a controller configured to receive said polling request and digitally sign said test verification data in response to said polling request.

Claim 101 (Canceled)

Claim 102 (Currently Amended) The system of claim ~~101~~100, wherein said rendering terminal processor is further configured to generate said test verification data randomly.

Claim 103 (Canceled)

Claim 104 (Previously Presented) The system of claim 100, wherein said rendering terminal and said mobile terminal each include a low power radio frequency interface.